Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A method of screening a software file for viral infection, the method comprising:
defining a database of known infected file signatures;
determining a signature for a file; and
screening that signature against the signatures contained in said database to determine if there is a match.

[c2] [Claim Reference]A method according to claim 1, wherein a match of signatures between the screened file and said database results in an action affecting the said screened file.

[c3] [Claim Reference]A method according to claim 1, wherein the result of a non matching signature between the screened file and said database results in an action affecting the said screened file.

[c4] [Claim Reference]A method according to claim 1, wherein the result of a non matching signature between the screened file and said database results in an action affecting the said database.

[c5] [Claim Reference]A method according to claim 1, wherein a match of signatures between the screened file and said

database results in an action affecting the database.

[c6] [Claim Reference]A method according to claim 1, wherein a match of signatures between the screened file and said database results in an alert or notification to a user of a local computer system.

[c7] [Claim Reference]A method according to claim 6, wherein the said computer system is connected via an electronic link to a remote central computer.

[c8] [Claim Reference]A method according to claim 2, wherein a said action is an electronic quarantine of said matched file.

[c9] [Claim Reference]A method according to claim 1, wherein said database is updated via an electronic link between a computer hosting the database, where the scanning of the file is performed, and a remote central computer.

[c10] [Claim Reference]A method according to claim 1, wherein said database contains a flag set in memory to quarantine said screened files.

[c11] [Claim Reference]A method according to claim 1, wherein said database contains a flag set in memory to release quarantined files.

[c12] [Claim Reference]A method according to claim 1, wherein

said database contains a flag set in memory to erase said files.

[c13] [Claim Reference]A method according to claim 10, wherein said flag can be updated by remote software via an electronic link to end user computers.

[c14] [Claim Reference]A method according to claim 11, wherein said flag can be updated by remote software via an electronic link to end user computers.

[c15] [Claim Reference]A method according to claim 12, wherein said flag can be updated by remote software via an electronic link to end user computers.

[c16] [Claim Reference]A method according to claim 10, wherein said flag can be updated by a network manager and flag updates made by the network manager are communicated to network end user computers where infected file virus screening is performed.

[c17] [Claim Reference]A method according to claim 11, wherein said flag can be updated by a network manager and flag updates made by the network manager are communicated to network end user computers where infected file virus screening is performed.

[c18] [Claim Reference]A method according to claim 12,

wherein said flag can be updated by a network manager and flag updates made by the network manager are communicated to network end user computers where infected file virus screening is performed.

[c19] [Claim Reference]A method according to claim 10, wherein the quarantined file is placed in a non-executable electronic container.

[c20] [Claim Reference]A method according to claim 1, wherein the user is a network manager and database updates made by the network manager are communicated to network end user computers where infected file virus screening is performed.

[c21] [Claim Reference]A method according to claim 1, wherein said step of determining a signature for the file and screening that signature comprises deriving a signature of the file and comparing the derived signature with signatures in the database.

[c22] Apparatus for screening a software file for viral infection, the apparatus comprising:
a memory storing a database of known infected file signatures; and
a data processor arranged to scan said file to determine whether or not the file has a signature corresponding to

one of the signatures contained in said database.

[c23] [Claim Reference]The apparatus according to claim 22, wherein, in order to determine whether or not the file has a signature corresponding to one of the signatures contained in said database, said data processor is arranged to derive a signature of the file and to compare the derived signature with signatures in the databases.

[c24] A computer memory encoded with executable instructions representing a computer program for causing computer system to:
maintain a database of known infected file signatures; and
determine whether or not the file has a signature corresponding to one of the signatures contained in said database.

[c25] [Claim Reference]A computer memory according to claim 24, wherein the computer program causes the files to be scanned to determine whether or not they contain a signature corresponding to one of signatures contained in the database.

[c26] [Claim Reference]The computer memory according to claim 24, wherein in order to determine whether or not the file has a signature corresponding to one of the sig-

natures contained in said infected file database, said computer program causes the computer system to derive a signature of the file and to compare the derived signature with signatures in the database.

[c27] [Claim Reference]A method according to claim 1, wherein a match condition causes an alert or notification to be sent electronically to the user of the local computer system hosting said database.

[c28] [Claim Reference]A method according to claim 1, wherein a match condition causes an alert or notification to be sent electronically to a network administrator of a remote server.

[c29] [Claim Reference]The apparatus according to claim 22, wherein, is a part of a network firewall device.

[c30] [Claim Reference]The apparatus according to claim 22, wherein, is a part of a network IDS (Intrusion Detection System).

[c31] [Claim Reference]The apparatus according to claim 22, wherein, is a part of a network IPS (Intrusion Prevention System).

[c32] [Claim Reference]The apparatus according to claim 22, wherein, is a part of a network packet sniffer software.

[c33] [Claim Reference]The apparatus according to claim 22, wherein, is a part of a PDA (Personal Digital Assistant).

[c34] [Claim Reference]The apparatus according to claim 22, wherein, is a part of a digital camera.

[c35] [Claim Reference]The apparatus according to claim 22, wherein, is a part of a cellular phone.

[c36] [Claim Reference]The apparatus according to claim 22, wherein, is a part of a wireless device.

[c37] [Claim Reference]The apparatus according to claim 22, wherein, is a part of a computer system comprising one or more CPUs (Central Processing Unit) and one or more memories.

[c38] [Claim Reference]A method according to claim 1, wherein the said database is a part of a bidirectional system for sending and receiving partial hash signatures.

[c39] [Claim Reference]A method according to claim 38, wherein partial hash signatures are sent and received through a bidirectional request protocol set to determine a percentage of said file used in hash computation.

[c40] [Claim Reference]A method according to claim 39, wherein the requested percentage is set by a dynamic

request protocol based on communication speed.

[c41] [Claim Reference]A method according to claim 39, wherein the requested percentage is set by a dynamic request protocol based on file size.

[c42] Apparatus for determining a partial file hash signature:
a memory storing a database of known infected file signatures; and
a memory storing a database of partial file signatures; and
a data processor arranged to scan said file incrementally and add file hash signatures, upon request, to said database of partial file signatures; and
to add said hash signatures, upon request, to said database of infected file signatures.

[c43] [Claim Reference]The apparatus according to claim 42, wherein the percentage scanned and imputed into said partial file signature database is set by a bidirectional electronic data protocol.

[c44] [Claim Reference]The apparatus according to claim 43, wherein the said bidirectional electronic data protocol contains a field of type contained in said protocol.

[c45] [Claim Reference]The apparatus according to claim 44, wherein the said protocol is communicated electronically

over a computer network.

[c46] [Claim Reference]The apparatus according to claim 42, wherein the said partial file hash signature is computed through reverse computation based on probability of a match condition between said partial file and said infected file signature database.

[c47] [Claim Reference]The apparatus according to claim 43, wherein the said bidirectional electronic data protocol contains a field of length contained in said protocol.

[c48] [Claim Reference]The apparatus according to claim 47, wherein the said field of length is communicating the numerical value of the percent of a hash computed.

[c49] [Claim Reference]The apparatus according to claim 42, wherein the said determination of partial file hash signatures is modified based on block size of end user system when compared to block size on a remote server.